Web Images Videos Maps News Shopping Gmail more ▾ Scholar Preferences | Sign in

Google scholar "intrusion detection" "application layer" Search Advanced Scholar Search

● Search only in Engineering, Computer Science, and Mathematics.

○ Search in all subject areas.

Scholar Articles excluding patents - 2004 include citations Create email al

[PDF] Snort-lightweight **intrusion detection** for networks
M Roesch - Proceedings of the 13th USENIX conference on ..., 1999 - usenix.org
... 229 Page 3. Snort – Lightweight **Intrusion Detection** for Networks Roesch How Is Snort Different From tcpdump? ... Snort decodes the **application layer** of a packet and can be given rules to collect traffic that has spe- cific data contained within its **application layer**. ...
Cited by 1632 - Related articles - View as HTML - All 44 versions

Intrusion detection in wireless ad-hoc networks
Y Zhang... - Proceedings of the 6th annual international ..., 2000 - portal.acm.org
... However, **intrusion detection** in the **application layer** is not only feasible, as discussed in the previous section, but also necessary because certain attacks, for example, an attack that tries to create an unauthorized access "back-door" to a service, may seem perfectly legiti- mate ...
Cited by 802 - Related articles - All 40 versions

Intrusion detection techniques for mobile wireless networks
Y Zhang, W Lee... - Wireless Networks, 2003 - Springer
... services. In the wireless networks, there are no firewalls to protect the services from attack. However, **intrusion detection** in the **application layer** is not only feasible, as discussed in the previ- ous section, but also necessary. Certain ...
Cited by 394 - Related articles - BL Direct - All 31 versions

Infrastructure for **intrusion detection** and response
D Schnackenberg, K Djahandari... - discex, 2000 - computer.org
... IDIP is an **application layer** protocol that coordinates intrusion tracking and isolation. IDIP systems are organized into IDIP communities (as shown in Figure 1). Each IDIP community is an administrative domain, with **intrusion detection** and response functions managed by a ...
Cited by 142 - Related articles - All 4 versions

Honeycomb: creating **intrusion detection** signatures using honeypots
C Kreibich... - ACM SIGCOMM Computer Communication ..., 2004 - portal.acm.org
... II. BACKGROUND A. **Intrusion Detection** Signatures The purpose of attack signatures is to describe the charac- teristic elements of attacks. ... Algorithm The philosophy behind our approach is to keep the system free of any knowledge specific to certain **application layer** protocols. ...
Cited by 342 - Related articles - BL Direct - All 65 versions

Testing network-based **intrusion detection** signatures using mutant exploits
G Vigna, W Robertson... - ... of the 11th ACM conference on ..., 2004 - portal.acm.org
... One may argue that the **intrusion detection** system may be considered to be the test suite and that the variations of an attack ... Mutation techniques can operate at several layers, the most significant of which are the network layer, the **application layer**, and the exploit layer. ...
Cited by 122 - Related articles - All 27 versions

[PDF] Active platform security through **intrusion detection** using naive bayesian network for

anomaly detection
AA Sebyala, T Olukemi... - London Communications Symposium, 2002 - Citeseer
... There are two main categories of **intrusion detection** techniques; Anomaly detection and Misuse detection. ... References [1] Ian W Marshal, ("An architecture for **application layer** active networking", IEE, London, 2000. [2] Ognjen Prnjat, et. ...
Cited by 39 - Related articles - View as HTML - All 5 versions

Adaptive neuro-fuzzy **intrusion detection** systems
S Chavan, K Shah, N Dave, S Mukherjee... - 2004 - computer.org
... SNORT is a libpcap-based sniffer and logger [3]. It is a cross- platform, lightweight **intrusion detection** tool that can be deployed to monitor small ... SNORT decodes the **application layer** of a packet and can be given rules to collect traffic that has specific data contained within its ...
Cited by 40 - Related articles - All 29 versions

Collaborative **intrusion detection** system (cids): A framework for accurate and efficient ids
YS Wu, B Foo, Y Mei... - 2003 - computer.org
... For this purpose, a system is divided into the network layer, the kernel layer and the **application layer**. ... We design and implement a system called the Collaborative **Intrusion Detection** System (CIDS) to demonstrate the feasibility of the idea. ...
Cited by 41 - Related articles - All 12 versions

Denial of service in sensor networks
AD Wood... - Computer, 2002 - ieeexplore.ieee.org
... An **intrusion-detection** system monitors a host or network for suspicious activity patterns such as those that match some preprogrammed or ... architecture encompasses several net- work layers, from a prioritized MAC layer to the query-event API just below the **application layer**. ...
Cited by 854 - Related articles - Library Search - BL Direct - All 8 versions

Operational experiences with high-volume network **intrusion detection**
H Dreger, A Feldmann, V Paxson... - Proceedings of the 11th ..., 2004 - portal.acm.org
... Next we recapitulate a recurring experience: in network **intrusion detection**, one faces a rather unusual trade-off between resource requirements and ... of state entries differs due to factors such as IP defragmenta- tion, TCP stream reassembly, and **application-layer** analysis, which ...
Cited by 82 - Related articles - All 24 versions

Protocol analysis in **intrusion detection** using decision tree
T Abbes, A Bouhoula... - ... Technology: Coding and ..., 2004 - ieeexplore.ieee.org
... **Intrusion detection** systems (IDS) employ protocol anal- ysis in order to understand the traffic and supervise the ex- ecution of some selected ... Our goal with the protocol analysis is to supervise the ex- ecution of **application layer** protocols and understand the nature of the traffic in ...
Cited by 42 - Related articles - All 16 versions

Measuring normality in HTTP traffic for anomaly-based **intrusion detection**
JM Estévez-Tapiador, P García-Teodoro... - Computer Networks, 2004 - Elsevier
... 4. A new stochastic approach for anomaly-based **intrusion detection** at the **application layer**. In this section, we present a new stochastic approach intended to improve on the general anomaly-based **intrusion detection** results provided by currently used techniques. ...
Cited by 41 - Related articles - All 8 versions

Learning rules for anomaly detection of hostile network traffic
MV Mahoney... - Data Mining, 2003. ICDM 2003. ..., 2003 - ieeexplore.ieee.org
... We tested LERAD using two data sets: the 1999 DARPA/Lincoln Laboratory **intrusion detection** evaluation (IDEVAL) [5], and 623 hours of traffic ... In the university traffic, all of the anomalies are due to idiosyncratic variations, mostly at the **application layer**, for example, generic ...
Cited by 93 - Related articles - All 41 versions

[PDF] Network traffic anomaly detection based on packet bytes
MV Mahoney - Proc. ACM-SAC. 2003 - Citeseer
... always use uppercase. • Evasion. Attackers may deliberately manipulate network protocols to hide an attack from an improperly coded **intrusion detection** system (IDS) monitoring the **application layer** [3, 11]. Such methods include ...
Cited by 146 - Related articles - View as HTML - All 46 versions

SCIDIVE: a stateful and cross protocol **intrusion detection** architecture for voice-over-IP environments
YS Wu, S Bagchi, S Garg, N Singh... - 2004 - computer.org
... Since VoIP systems use multiple **application layer** protocols, horizontal cross-protocol correlation is required. ... Our goal in the paper is to provide an architecture suited to **intrusion detection** in VoIP systems and show the feasibility of the architecture by demonstrating its behavior ...
Cited by 66 - Related articles - All 20 versions

Design and implementation of a TCG-based integrity measurement architecture
R Sailer, X Zhang, T Jaeger... - Proceedings of the 13th ..., 2004 - portal.acm.org
... to extend the TCG trust measurement concepts to dynamic executable content from the BIOS all the way up into the **application layer**. ... 8. [8] G. Kim and E. Spafford, "Experience with Tripwire: Using Integrity Checkers for **Intrusion Detection**," in System Administration, Networking ...
Cited by 551 - Related articles - All 18 versions

[PDF] Deciphering detection techniques: Part ii anomaly-based **intrusion detection**
F Gong - White Paper, McAfee Security, 2003 - secure.mcafee.com
... When attacks have progressed beyond control channel activity, anomaly-based **intrusion detection** is the only reliable means for detection in the ... This includes network and transport layer protocol anomalies in layers 3-4 and **application layer** protocol anomalies in layers 6-7 ...
Cited by 27 - Related articles - View as HTML - All 45 versions

Intrusion prevention system design
X Zhang, C Li... - 2004 - computer.org
... 3) Filtering rules of the firewall are usually very simple, so firewall can not prevent attack coming from **application layer**, and can not prevent virus also. ... So **Intrusion Detection** module in the firewall is secondary, and its function is limited, only alert to manager. ...
Cited by 40 - Related articles - All 4 versions

[BOOK] Applying mobile agents to **intrusion detection** and response
WA Jansen... - 1999 - Citeseer
... One of the greatest benefits of MAs is the implementation of interoperability at the **application layer**. ... COTS interoperability may also be facilitated via the use of Agent Communication Languages (ACL) designed for network security testing and **intrusion detection** domains. ...
Cited by 114 - Related articles - View as HTML - Library Search - All 45 versions

[PDF] PHAD: Packet header anomaly detection for identifying hostile network traffic
M Mahoney... - Florida Institute of Technology technical report CS ..., 2001 - Citeseer
... Horizon (1998) and Ptacek and Newsham (1998) describe techniques for attacking or evading an **application layer** IDS that would produce anomalies at the layers below. ... For example, in the DARPA **intrusion detection** data set (Lippmann et al. ...
Cited by 106 - Related articles - View as HTML - All 8 versions

Architectures for intrusion tolerant database systems
P Liu - Computer Security Applications Conference, 2002. ..., 2002 - ieeexplore.ieee.org
... Multi-layer **intrusion detection** is usually necessary for detection accuracy. First, proofs from **application layer**, session layer, transaction layer, process layer, and system call layer should be synthesized to do in- trusion detection. ...

Cited by 95 - Related articles - All 15 versions

A specification-based **intrusion detection** system for AODV
CY Tseng, P Balasubramanyam, C Ko... - Proceedings of the ..., 2003 - portal.acm.org
... distributed **intrusion detection** and response framework for MANET. Anomaly detection is the primary ID approach discussed, including anomalies in routing updates, abnormalities at the MAC layer (number of channel requests, etc.) and at the mobile **application layer** (number **...**
Cited by 144 - Related articles - All 11 versions

Towards nic-based **intrusion detection**
M Otey, S Parthasarathy, A Ghoting, G Li... - Proceedings of the ..., 2003 - portal.acm.org
... As a result, several data stream processing algorithms are rendered inapplicable for network **intrusion detection** un- der real-time processing requirements. **...** see figure 2) is loosely based on one of the models used in the non-stationary **application layer** anomaly detection (ALAD **...**
Cited by 34 - Related articles - All 14 versions

An environment for security protocol **intrusion detection**
A Yasinsac - Journal of Computer Security, 2002 - IOS Press
... way. The security of the information provided by trusted services at the **application layer** is dependent on security protocols. **...** We begin by giving the background work in security protocol verification and **intrusion detection**. The **...**
Cited by 23 - Related articles - BL Direct - All 6 versions

[BOOK] Computer **intrusion detection** and network monitoring: a statistical viewpoint
DJ Marchette - 2001 - books.google.com
... The section on **intrusion detection** is split into network and host monitoring. **...** It passes it up to the IP.layer, which passes it to the protocol layer and finally to the **application layer**, where the email program (analogy: the local mail carrier) finally reads the "john.doe" of the email **...**
Cited by 99 - Related articles - Library Search - All 8 versions

Transport and application protocol scrubbing
GR Malan, D Watson, F Jahanian... - ... Joint Conference of the ..., 2000 - ieeexplore.ieee.org
... A. TCPnP Ambiguities and ID Evasion Sophisticated attacks can utilize protocol ambiguities between a network **intrusion detection** system and an end-host to **...** Since TCP is a reli- able byte-stream service that delivers its data to the **application layer** in order, both the end-host **...**
Cited by 69 - Related articles - BL Direct - All 26 versions

Learning nonstationary models of normal network traffic for detecting novel attacks
MV Mahoney... - Proceedings of the eighth ACM SIGKDD ..., 2002 - portal.acm.org
... Second, an attacker may deliberately use malformed or unusual packets to hide attacks from an IDS **application layer**. **...** Unfortunately, this is a common problem. For example, Handley et. al. [7] studied four commercial **intrusion detection** systems and found that none of them ...
Cited by 226 - Related articles - All 15 versions

eXpert-BSM: A host-based **intrusion detection** solution for Sun Solaris
U Lindqvist... - acsac, 2001 - computer.org
... **Application-layer** encryption of network traffic is be- coming more common and user transparent thanks to tech- nology such as SSL-enabled **...** positive step for- ward in communications integrity and the prevention of data theft, it makes network-based **intrusion detection** more diffi **...**
Cited by 41 - Related articles - All 28 versions

Distributed firewalls
SM Bellovin - Journal of Login, 1999 - usenix.org
... It is most natural to think of this happening at the network or the transport layer, but policies and enforcement can equally well apply to the **application layer**. For **...** problem.

For now, a distributed **intrusion-detection** system would be useful. ...
Cited by 161 - Related articles - All 49 versions

Efficient minimum-cost network hardening via exploit dependency graphs
S Noel, S Jajodia, B O'Berry... - 2003 - computer.org
... details). Similarly, we model the combination of **application-layer** trust and physical-layer connectivity as simply **application-layer** trust. ... services. **Application- layer** trust relationships further restrict NFS and NIS domain access. ...
Cited by 134 - Related articles - All 17 versions

[PDF] Live traffic analysis of TCP/IP gateways
PA Porras... - NDSS, 1998 - isoc.org
... These monitors demonstrate a streamlined **intrusion-detection** design that combines signature analysis withstatistical pro l- i ng to provi de l ocal i zed real ... ng corrupti on or forgery of l egi ti mate tra cin an at- tempt to negativelya ect routing services, **application- layer** services, or ...
Cited by 129 - Related articles - View as HTML - All 2 versions

Intrusion detection system for high-speed network
W Yang, BX Fang, B Liu... - Computer Communications, 2004 - Elsevier
... packet capture, and efficient data analysis based on application protocol analysis and a multi-rule based **intrusion detection** engine implemented ... Third, an **application-layer** protocol analysis and reassembling mechanism reduce the false alarm rate and reinforces the NIDS itself ...
Cited by 14 - Related articles

Passive visual fingerprinting of network attack tools
G Conti... - Proceedings of the 2004 ACM workshop on ..., 2004 - portal.acm.org
... which can be used for such activities as detecting Honeynets[25] and insertion and evasion attacks to bypass **intrusion detection** systems[26]. ... 3.2.1.4 **Application Layer Application layer** headers and data provide a great deal of information about the nature of attacks, but due to ...
Cited by 59 - Related articles - All 9 versions

Evaluation of the diagnostic capabilities of commercial **intrusion detection** systems
H Debar... - Recent Advances in **Intrusion Detection**, 2002 - Springer
... Misunderstanding of the protocol states or properties. Sometimes, vul- nerabilities are only applicable to certain states of the **application layer** proto- cols. ... Sometimes, protocols encode data, hiding the information from the **intrusion-detection** system and inducing false positives. ...
Cited by 28 - Related articles - BL Direct - All 12 versions

A fast string-matching algorithm for network processor-based **intrusion detection** system
RT Liu, NF Huang, CH Chen... - ACM Transactions on ..., 2004 - portal.acm.org
... Generally two main methods are used for **intrusion detection**, namely pattern matching and statistical analysis. ... The increase in network utilization and the weekly expansion in number of critical **application layer** exploits means NIDSs designers must develop ways to accelerate ...
Cited by 68 - Related articles - All 3 versions

A dynamic honeypot design for **intrusion detection**
I Kuwatly, M Sraj, Z Al Masri... - 2004 - computer.org
... III- RELATED WORK The honeypot technology is an attempt to overcome the shortcomings of **intrusion detection** systems. A. Definition ... KFSensor simulates system services at the **application layer**, thus enabling it to use Windows security mechanisms and libraries. ...
Cited by 23 - Related articles - All 9 versions

DECIDUOUS: decentralized source identification for network-based intrusions
HY Chang, R Narayan, SF Wu... - ... Management for the ..., 1999 - ieeexplore.ieee.org
... protocol layers. For example, in DECIDUOUS, it is possible for a network-layer security

control protocol (eg, IPSEC) to collaborate with an **application-layer intrusion detection** system module (eg, IDS for the SNMP engine). In this **...**
Cited by 46 - Related articles

Shield: Vulnerability-driven network filters for preventing known vulnerability exploits
HJ Wang, C Guo, DR Simon... - ACM SIGCOMM ..., 2004 - portal.acm.org
... To this end, we have de- signed a Shield framework that lies between the **application layer** and the transport layer and **...** session, and performs application-message-based inspection rather than packet-level inspection, as used by some Network **Intrusion Detection** or Prevention **...**
Cited by 244 - Related articles - BL Direct - All 36 versions

[PDF] Building adaptive and agile applications using **intrusion detection** and response
JP Loyall, P Pal, R Schantz... - Proceedings of NDSS, 2000 - isoc.org
... simple custom developed IDS, and application-specified **intrusion detection** are all integrated to provide intrusion awareness and adaptive **...** An application seamlessly interfacing to multiple IDSs, enabling the IDSs to cooperate through the **application layer** and increasing **...**
Cited by 20 - Related articles - View as HTML - All 3 versions

Implementing the **intrusion detection** exchange protocol
T Buchheim, M Erlinger, B Feinstein, G Matthews... - acsac, 2001 - computer.org
... BEEP TCP IP Ethernet, ATM, etc. Figure 2: BEEP's Position in TCP/IP Protocol Stack. 7 **Intrusion Detection** Exchange Protocol (IDXP) **...** When one or more inter- mediate hops are required, the protocol needs to set up an **application-layer** tunnel across those hops. **...**
Cited by 14 - Related articles - All 9 versions

Detecting computer and network misuse through the production-based expert system toolset (P-BEST)
U Lindqvist... - sp, 1999 - computer.org
... For more than a decade, earlier versions of P-BEST have been used in **intrusion detection** research and in the development of some of the most well- known **intrusion detection** systems, but this is the first time the principles and language of P-BEST are described to a wide **...**
Cited by 280 - Related articles - BL Direct - All 45 versions

TJIDS: an **intrusion detection** architecture for distributed network
Q Xue, J Sun... - Electrical and Computer Engineering, ..., 2003 - ieeexplore.ieee.org
... 3.1 Encryption Algorithm Design in Agent Communication It is very important to encrypt communication information between agents for the security of the network **intrusion detection** system itself. **...** So we design a set of Agent **Application Layer** Communication Protocol (AALCP). **...**
Cited by 15 - Related articles

Sleepy watermark tracing: An active network-based intrusion response framework
X Wang, DS Reeves, SF Wu... - ... (IFIP/Sec'01), June 11-13, ..., 2001 - books.google.com
... Page 396. 378 Part Nine Network Security and **Intrusion Detection** SWT tracing. **...** Therefore, watermark belongs to the **application layer** and is application-specific. One challenge in generating watermark is how to make watermarks invisible to end-users. **...**
Cited by 87 - Related articles - All 24 versions

A model for evaluating IT security investments
H Cavusoglu, B Mishra ... - Communications of the ..., 2004 - portal.acm.org
... What is the trade-off between preventive controls, such as a firewall, and detective controls, such as an **Intrusion Detection** System (IDS). We propose a comprehensive analytical model to evaluate security investment decisions. **...** The **Application layer** mechanism uses proxies. **...**
Cited by 149 - Related articles - BL Direct - All 10 versions

Self-organized network-layer security in mobile ad hoc networks

H Yang, X Meng ... - Proceedings of the 1st ACM workshop on ..., 2002 - portal.acm.org
... route entries are the same, and the hop count in the new route entry is one larger than the hop count in the cached route entry announced by Y . If the routing update is not cor- rect, the RREP packet is dropped and node S broadcasts a SID(Single **Intrusion Detection**) packet to ...
Cited by 196 - Related articles - All 19 versions

Interfacing trusted applications with **intrusion detection** systems
M Welz... - Recent Advances in **Intrusion Detection**, 2001 - Springer
... Most network-based **intrusion detection** systems make use of this method. ... An example of such a system would be the **application layer** proxies of TIS's firewall toolkit [19] or the audit trail of an operating system which records the system calls made by an application. ...
Cited by 20 - Related articles - BL Direct - All 9 versions

Anomaly **intrusion detection** in dynamic execution environments
H Inoue... - Proceedings of the 2002 workshop on New ..., 2002 - portal.acm.org
... We call this approach "dynamic sandboxing." By gathering information about applications' behavior usually unavail- able to other anomaly **intrusion-detection** systems, dynamic sandboxing is able to detect anomalies at the **application layer**. ...
Cited by 31 - Related articles - All 9 versions

The prediction role of hidden markov model in **intrusion detection**
F Gao, J Sun... - Electrical and Computer Engineering, ..., 2003 - ieeexplore.ieee.org
... Therefore, we present an approach to resolve this problem. We mainly apply this approach to **intrusion detection** on **Application Layer**. However, it can be adapted for the **intrusion detection** on Network Layer and Transfer Layer. Some results are also given in this paper. ...
Cited by 8 - Related articles

[PDF] Providing robust and ubiquitous security support for mobile ad hoc networks
H Luo, S Lu... - Proceeding of The 9th International Conference on ..., 2001 - Citeseer
... The assumption of local de- tection mechanisms is based on the observation that although **intrusion detection** in ad hoc networks is generally ... network layer Smurf and Teardrop, transport layer TCP flooding and SYN flooding, and numerous attacks in the **application layer** [15]. ...
Cited by 598 - Related articles - View as HTML - All 32 versions

A framework for malicious workload generation
J Sommers, V Yegneswaran... - Proceedings of the 4th ..., 2004 - portal.acm.org
... benchmarking tool that enables as- sessment of quality of service degradation (the effect of mal-traffic on good traffic) and resilience of middleboxes and network **intrusion detection** systems (NIDS) over a ... These could either be at the network layer or at the **application layer**. ...
Cited by 50 - Related articles - All 17 versions

Stopping intruders outside the gates
LD Paulson - Computer, 2002 - ieeexplore.ieee.org
... The traditional approach: **Intrusion detection Intrusion-detection** systems (IDSs) have been a standard approach to net- work security for the past couple of ... Diane Fraiman, the company's vice president of mar- keting, said 80 percent of attacks orig- inate in the **application layer**. ...
Cited by 22 - Related articles - BL Direct - All 5 versions

Attacking DDoS at the source
J Mirkovic, G Prier... - Network Protocols, 2002. ..., 2002 - ieeexplore.ieee.org
... The kernel module delay stays sta- ble regardless of the imposed load and is between 1 and 10 μs. The **application layer** delay increases as the hash tables fill up, since some time is spent keeping them reasonably empty so that new records can be inserted. ...
Cited by 293 - Related articles - All 3 versions

[PDF] **Intrusion detection** system (IDS) product survey
KA Jackson - Los Alamos National Laboratory, Los Alamos, NM, ..., 1999 - Citeseer
... 06/25/99 **INTRUSION DETECTION** SYSTEM (IDS) PRODUCT SURVEY ... ii Version 2.1 4.10 REACTIVE **INTRUSION DETECTION** ..... 65 4.11 REALSECURE..... ...
Cited by 43 - Related articles - View as HTML - All 9 versions

Anomaly detection methods in wired networks: a survey and taxonomy
JM Estevez-Tapiador, P Garcia-Teodoro... - Computer ..., 2004 - Elsevier
... Keywords: Anomaly detection; Network **intrusion detection**; Computer and network security; Network management. Article Outline. 1. Introduction 1.1. ... Case study V: specification-based protocol anomaly detection 6. **Application-layer** anomaly detection: payload inspection 6.1. ...
Cited by 48 - Related articles - All 7 versions

Network **Intrusion Detection** Techniques Based on Protocol Analysis [J]
JRLLH Jinpeng - Computer Engineering and Applications, 2003 - en.cnki.com.cn
... analysis technique based on state transition,it proposes an **intrusion detection** technique that takes full advantage of the protocol state information for detecting intrusion.It can effectively analyze protocols at various layers of network including **application layer** protocols and can ...
Cited by 7 - Related articles - Cached

[PDF] Design and implementation of a string matching system for network **intrusion detection**
FPGA-based bloom filters
S Dharmapurikar, M Attig... - ... University in St. Louis, Tech. Rep ..., 2004 - Citeseer
... For applications like network **intrusion detection**, these updates are relatively less frequent than the actual query process it- self. ... Packets on the link are parsed by the protocol wrappers [2] and the **application layer** data is presented to the scanner module. ...
Cited by 30 - Related articles - View as HTML - All 8 versions

HMM profiles for network traffic classification
C Wright, F Monrose... - ... of the 2004 ACM workshop on ..., 2004 - portal.acm.org
... General Terms Security, Measurement Keywords masquerade detection, **intrusion detection**, behavioral mod- eling 1 ... emit. Most **application layer** protocols do have such struc- ture, which is largely defined by RFC specifications. ...
Cited by 56 - Related articles - All 3 versions

Honeypot: a supplemented active defense system for network security
F Zhang, S Zhou, Z Qin... - Parallel and Distributed ..., 2003 - ieeexplore.ieee.org
... The third layer is log component which logs all the activities of the honeypot OS in **application layer**. Log ... attacks. The other contribution to **intrusion detection** is that it can reduce both false positive rate and false negative rate. ...
Cited by 24 - Related articles - All 3 versions

Web application security assessment by fault injection and behavior monitoring
YW Huang, SK Huang, TP Lin... - Proceedings of the 12th ..., 2003 - portal.acm.org
Page 1. Web Application Security Assessment by Fault Injection and Behavior Monitoring Yao-Wen Huang, Shih-Kun Huang, and Tsung-Po Lin Institute of Information Science, Academia Sinica Nankang 115 Taipei, Taiwan {ywhuang,skhuang,lancelot} @iis.sinica.edu.tw ...
Cited by 157 - Related articles - All 11 versions

A novel distributed **intrusion detection** model based on mobile agent
S Zhicai, J Zhenzhou... - Proceedings of the 3rd ..., 2004 - portal.acm.org
... as an **application-layer** proxy. It allows authorized users to access services through a frewall. So two different subnet monitors can exchange message safely. These BEEP protocols are called by the communication control module of IDSs. So **intrusion detection** entities can ...
Cited by 11 - Related articles - All 2 versions

[PDF] Bro: An open source network **intrusion detection** system
R Sommer - Proceedings of the 17. DFN-Arbeitstagung über ..., 2003 - Citeseer
... Traditionally, two approaches to network **intrusion detection** are differentiated: a system using anomaly-detection relies on a definition of normal network ... On the **application layer**, it implements a variety of protocol-specific analyzers, eg for HTTP, SMTP, DNS and many others. ...
Cited by 10 - Related articles - View as HTML - All 6 versions

The design of a distributed network **intrusion detection** system IA-NIDS
Q Xue, LL Guo... - Machine Learning and Cybernetics, ..., 2003 - ieeexplore.ieee.org
... IA-NIDS is different from the detection system we mentioned before in these aspects: (1) It introduces Cluster to make parallel reassembly **intrusion detection** on the **application layer**. (2) It introduces distributed agent system ...
Cited by 5 - Related articles

[PDF] Scampi-a scaleable monitoring platform for the internet
J Coppens, E Markatos, J Novotny... - Proceedings of the 2nd ..., 2004 - Citeseer
... The monitoring layer, belonging to a single Internet Service Provider (ISP), provides end-to-end QoS statistics of the observed network to the **application layer**. ... NDISs (Network **Intrusion Detection** Systems) are an important part of any modern network security architec- ture. ...
Cited by 29 - Related articles - View as HTML - All 14 versions

[BOOK] **Intrusion detection** systems with Snort: advanced IDS techniques using Snort, Apache MySQL, PHP, and ACID
RU Rehman - 2003 - books.google.com
... Page 21. What is **Intrusion Detection**? 7 1.1.1.4 Signatures Signature is the pattern that you look for inside a data packet. ... For example, you can find signatures in the IP header, transport layer header (TCP or UDP headerl and/or **application layer** header or payload. ...
Cited by 29 - Related articles - Library Search - All 4 versions

Anomaly detection in IP networks
M Thottan... - Signal Processing, IEEE Transactions on, 2003 - ieeexplore.ieee.org
... The protocol provides a mechanism to communicate between the manager and the agent. A single SNMP manager can monitor hundreds of SNMP agents that are located on the network devices. SNMP is implemented at the **application layer** and runs over the UDP. ...
Cited by 208 - Related articles - BL Direct - All 21 versions

[PDF] Detecting novel attacks by identifying anomalous network packet headers
M Mahoney... - Florida Institute of Technology Technical Report ..., 1999 - Citeseer
... We got good performance because the important fields for **intrusion detection** have a small r, so that hash collision are rare for ... Out-of-spec attacks (according to our unofficial classification) are shown in parenthesis, with the **application layer** protocol that those attacks exploit. ...
Cited by 44 - Related articles - View as HTML - All 7 versions

Anomaly Network **Intrusion Detection** System Based on Data Mining [J]
S Shi-jie, HU Hua-ping, HU Xiao-lei... - Computer ..., 2003 - en.cnki.com.cn
... Anomaly Network **Intrusion Detection** System Based on Data Mining. ... some data mining algorithms, presentd a classification method of IDS based on data mining, and described the process of data mining application in anomaly NIDS from network layer and **application layer**. ...
Cited by 6 - Related articles - Cached

Visualisation for **Intrusion Detection**
S Axelsson - Computer Security--ESORICS 2003, 2003 - Springer
... network traffic and alarms from a network of **intrusion detection** sensors as glyphs onto a stylised map of the network. As such their approach is very different from ours, in that we don't map the traffic as such, but rather try and visualise meta data from the **application layer** in a ...

Cited by 23 - Related articles - BL Direct - All 11 versions

[PDF] Boundary detection in tokenizing network application payload for anomaly detection
R Vargiya... - Workshop on Data Mining for Computer Security, 2003 - Citeseer
... rationale for selecting the optimal pattern length, which has a major influence on the detection capabilities of the **intrusion detection** system ... boundaries are statistical, our approach is independent of the language or in our case, independent of the protocol of the **application layer**. ...
Cited by 24 - Related articles - View as HTML - All 4 versions

GRIP: A reconfigurable architecture for host-based gigabit-rate packet processing
P Bellows, J Flidr, T Lehman... - ... . 10th Annual IEEE ..., 2002 - ieeexplore.ieee.org
... reconfigurable comput- ing. These range from **intrusion detection** at the link layer and encryption at the network layer (IPSec) to protocol pro- cessing at the transport layer and parallel computing at the **application layer**. The goal of ...
Cited by 33 - Related articles - All 15 versions

The Evolution of **Intrusion Detection** Systems--The Next Step
R Barber - Computers & Security, 2001 - Elsevier
... Nobody is suggesting that the solution is perfect or that **Intrusion Detection** Systems are complete as they stand, but it does show that there is a ... It should also be able to detect and prevent **application layer** attacks that should be performed on or maybe just in front of application ...
Cited by 11 - Related articles - All 4 versions

[PDF] Optimizing pattern matching for **intrusion detection**
M Norton - white paper, Sourcefire Inc, 2004 - Citeseer
... NORT is an open source **Intrusion Detection** System that relies heavily on the Aho-Corasick multi-pattern search engine. ... searching for intruders by looking for specific values in the network headers and by performing a search for known patterns in the **application layer** data. ...
Cited by 40 - Related articles - View as HTML - All 3 versions

[PDF] Design of an intrusion-tolerant **intrusion detection** system
M Dacier - Research Report, Maftia Project, 2002 - Citeseer
... Malicious- and Accidental-Fault Tolerance for Internet Applications Design of an Intrusion-Tolerant **Intrusion Detection** System M. Dacier (Editor) IBM Zurich Research Laboratory ... Page 3. Design of an intrusion-tolerant **intrusion detection** system i Table of contents ...
Cited by 25 - Related articles - View as HTML - All 5 versions

Wireless **intrusion detection** and response: a classic study using main-in-the-middle attack
TR Schmoyer, YX Lim... - ... Conference, 2004. WCNC. ..., 2004 - ieeexplore.ieee.org
... Libnet is a network library used to create data-link, network and **application layer** protocol headers and transmit the resultant frames. ... The toolkit was divided into separate modules, each designed to provide specific functions for **intrusion detection** and response. ...
Cited by 13 - Related articles

[PDF] Survivability-over-security: Providing whole system assurance
W Yurcik, D Doss... - Information Survivability Workshop, 2000 - Citeseer
... Applications and **application-layer** protocols have been found to interact in unexpected ways with these new layer-violating (LV) network devices (which break the end-to-end model) such as network address translators, firewalls, proxies, **intrusion detection**, and differentiated ...
Cited by 12 - Related articles - View as HTML - All 7 versions

N3: A geometrical approach for network **intrusion detection** at the **application layer**
JM Estévez-Tapiador, P García-Teodoro... - ... Science and Its ..., 2004 - Springer
Abstract. In this work, a novel approach for the purpose of anomaly- based network **intrusion detection** at the **application layer** is presented. The problem of identifying anomalous payloads

is addressed by using a technique based on the modelling of short sequences of ...
Cited by 3 - Related articles - BL Direct - All 4 versions

[PDF] Linux security module framework
C Wright, C Cowan, J Morris, S Smalley... - Ottawa Linux ..., 2002 - Citeseer
... The netlink_send () hook is used to store the **application layer** security state. The netlink_recv () hook is used to retrieve the stored security state as the packet is received by the destination kernel module and mediate final delivery. ... LIDS (Linux **Intrusion Detection** Sys- tem ...
Cited by 47 - Related articles - View as HTML - All 46 versions

Packet trace manipulation rramework for test labs
A Rupp, H Dreger, A Feldmann... - Proceedings of the 4th ..., 2004 - portal.acm.org
... 2.1 Network **Intrusion Detection** A common approach to evaluating NIDSs uses captured packet traces to create realistic network work-loads. ... or reordered; at the transport layer, an end-point's round-trip-time estima- tion may no longer be valid; at the **application layer**, it is ...
Cited by 18 - Related articles - All 22 versions

Detecting anomalous network traffic with self-organizing maps
M Ramadas, S Ostermann... - ... Advances in **Intrusion Detection**, 2003 - Springer
... For this, the signature-based **intrusion detection** system SNORT is run on the dumpfile, and connections reported by SNORT as intrusive are removed. ... The HTTP Tunnel program creates **application-layer** HTTP tunnels between two hosts, and lets any type of traffic to be run on ...
Cited by 103 - Related articles - Library Search - BL Direct - All 47 versions

[PDF] Quickprop neural network ensemble forecasting framework for a database intrusion predi system
P Ramasubramanian... - Neural Information Processing-Letters ..., 2004 - Citeseer
... works were focused largely on network-based **intrusion detection** [7][8] and host-based **intrusion detection** [4][5]. These **intrusion detection** systems do not work at the **application layer**, which can potentially offer more accurate and precise detection for the targeted application. ...
Cited by 17 - Related articles - View as HTML - All 4 versions

[PDF] The use of attack trees in assessing vulnerabilities in SCADA systems
E Byres, M Franz... - International Infrastructure Survivability ..., 2004 - ida.liu.se
... These systems were selected as a starting point since their underlying **application layer** protocol is both one ... Furthermore, detection of this type of attack is highly unlikely as few SCADA systems deploy any form of **intrusion detection** system and the direct impact to operations ...
Cited by 28 - Related articles - View as HTML - All 8 versions

Trust-based routing for ad-hoc wireless networks
AA Pirzada, A Datta... - Networks, 2004.(ICON ..., 2004 - ieeexplore.ieee.org
... However, as the routes retrieved from the cache are based the **application layer** of source nodes. upon a minimal trust threshold, we see a control packet ... We recommend using **Intrusion Detection** systems such as those proposed hy Zhang et al. [14] and Kachirski et al. ...
Cited by 33 - Related articles

A framework for analyzing e-commerce security
S Kesh, S Ramanujan... - Information management & ..., 2002 - emeraldinsight.com
... Host-based **intrusion detection** systems parse system logs and monitor user logins. ... Because of this, it is transparent to all users. While many applications may have their own security protocols, IPsec works at the network layer and can work with the **application layer** protocols. ...
Cited by 21 - Related articles - BL Direct - All 7 versions

Issues in high-speed internet security
P Jungck, SSY Shim - Computer, 2004 - computer.org

... Many firewalls left the port it attacked open to provide a service, and most **intrusion detection** systems left that port unmonitored. ... Full packet inspection involves fully interrogating the additional **application layer** headers and making correlative analysis of the data as a structured ...
Cited by 21 - Related articles - BL Direct - All 6 versions

Characteristics of role-based access control
V Gligor - Proceedings of the first ACM Workshop on Role-based ..., 1996 - portal.acm.org
... This is possible because **intrusion detection** would also have to be performed at the same low level as that of access control administration. ... [HAM1921 Deborah Hamilton, "**Application Layer** Security Requirements of a Medical Information System," Proceedings of the 15th NIST ...
Cited by 30 - Related articles - All 3 versions

Models for monitoring and debugging tools for parallel and distributed software
DC Marinescu, JE Lumpp Jr, TL Casavant... - Journal of Parallel and ..., 1990 - Elsevier
... layer will be built up from a standard library of functions to support the current **Application layer**, while the **Application layer** will be ... **Intrusion detection** is the direct result of the need to incorporate levels of the reactive process within the same processor that is supporting the active ...
Cited by 75 - Related articles - All 7 versions

[PDF] The Gigascope stream database
C Cranor, T Johnson, O Spatscheck... - Data Engineering, 2003 - Citeseer
... period, usually only the network protocol headers are stored, which frustrates analyses which use the **application layer** headers of the ... **Intrusion detection**: Network **intrusion detection** can be accomplished by expressing intrusion rules as GSQL queries and feeding the result ...
Cited by 39 - Related articles - View as HTML - All 22 versions

[PDF] Detecting intrusions in security protocols
A Yasinsac - ... of first workshop on **Intrusion Detection** Systems, in the ..., 2000 - Citeseer
... way. The security of the information provided by trusted services at the **application layer** is dependent on security protocols. ... We begin by giving the background work in security protocol verification and **intrusion detection**. The ...
Cited by 12 - Related articles - View as HTML - All 8 versions

Defining an adaptive software security metric from a dynamic software failure tolerance measur
J Voas, A Ghosh, G McGraw... - ..., 1996. COMPASS'96, ..., 1996 - ieeexplore.ieee.org
... Even patching this flaw in sendmail does not solve the problem of intrud- ers using other non-standard mail headers or exploiting other **application-layer** program vulnerabilities. ... **Intrusion detection** will be accomplished using a predicate-based intrusion specifi- cation language. ...
Cited by 48 - Related articles - All 8 versions

[PDF] Attack-class-based analysis of **intrusion detection** systems
D Alessandri - ... of Newcastle upon Tyne, Newcastle, UK, 2004 - homepage.swissonline.ch
Page 1. Attack-Class-Based Analysis of **Intrusion Detection** Systems Dominique Alessandri May 2004 Ph.D. Thesis ... School of Computing Science Page 2. Page 3. Abstract Designers of **intrusion detection** systems are often faced with the problem that their design fails ...
Cited by 16 - Related articles - View as HTML - Library Search - All 2 versions

[PDF] Defining digital forensic examination and analysis tools
B Carrier - Digital Research Workshop II, 2002 - Citeseer
... ASCII .H TML Files . Windows Registry . Network Packets . **Intrusion Detection** System (IDS)alerts . Source Code ... The second layer is the file system layer that translates the sector contents to files. The third layer is the **application layer** that translates the file content to 5 Page 6. ...
Cited by 91 - Related articles - View as HTML - All 32 versions

Dissecting Snort, tool for **intrusion detection** [J]

QI Jian-dong, TAO Lan... - Computer Engineering and ..., 2004 - en.cnki.com.cn
... Hunan University, Changsha 410082;The Research of Multi-pattern Matching Algorithm in Network **Intrusion Detection** System[J ... Engineering,Jiangsu University,Zhenjiang 212013,China);Research and implement of honeypot framework for **application layer's** unknown attacks[J ...
Cited by 5 - Related articles - Cached

Coordination of security levels for Internet architectures
EB Fernandez - dexa, 1999 - computer.org
... Current systems incorporate a variety of mechanisms to thwart attackers, eg, cryptographic protocols, **intrusion detection** methods, authorization systems, etc. ... At the **application layer** we can define authorizations using the conceptual model of the system and Role-Based Access ...
Cited by 16 - Related articles - All 7 versions

Timing-sync protocol for sensor networks
S Ganeriwal, R Kumar... - Proceedings of the 1st ..., 2003 - portal.acm.org
... The applications envisioned for sensor networks vary from monitoring inhospitable habitats and disaster areas to operating indoors for **intrusion detection** and equipment ... There is time spent in actually constructing the packet at the **application layer**, after which it is passed to the ...
Cited by 939 - Related articles - Library Search - All 42 versions

Efficacy of misuse detection in ad hoc networks
D Subhadrabandhu, S Sarkar... - Sensor and Ad Hoc ..., 2004 - ieeexplore.ieee.org
... An obvious IDS placement strategy (host **intrusion detection** or HID) [16] for adhoc networks is to execute the IDS at only the destinations of the sessions, eg destinations 1, 2 in figure 1. Here, a node executes the IDS at its **application layer**, and can therefore analyze only the ...
Cited by 20 - Related articles - All 8 versions

Protocol scrubbing: network security through transparent flow modification
D Watson, M Smart, GR Malan... - IEEE/ACM Transactions ..., 2004 - portal.acm.org
... A. TCP Ambiguities and ID Evasion Sophisticated attacks can utilize differences in the processing of packets between a network **intrusion detection** system and ... Since TCP is a reliable byte- stream service that delivers data to the **application layer** in order, both the end host and ...
Cited by 43 - Related articles - BL Direct - All 15 versions

A Framework for Understanding Vulnerabilities in Firewalls Using a Dataflow Model of Firewall Internals1
M Frantzen, F Kerschbaum, EE Schultz... - Computers & Security, 2001 - Elsevier
... Deriving a generic model of **Application Layer** filtering is futile. ... An often-overlooked feature is the ability to make a copy of a packet, then send the copy out to an isolated network for **intrusion detection** and split logging. Outbound Filtering. ...
Cited by 39 - Related articles - All 3 versions

[PDF] What do we mean by Network Denial of Service
C Shields - Proceedings of the 2002 IEEE Workshop on ..., 2002 - Citeseer
... Needham was the first to examine the effects of denial- of-service attacks at the **application layer**, focusing pri- marily on end-to-end solutions ... denial-of-service at- tacks was taken by Ptacek and Newsham [30] in their dis- cussion of methods of foiling **intrusion detection** systems. ...
Cited by 33 - Related articles - View as HTML - All 4 versions

[PDF] Windows performance monitoring and data reduction using watchtower
M Knop, J Schopf... - 11th IEEE Symposium on High-Performance ..., 2002 - Citeseer
... **Intrusion detection** Unusual behavior could be detected using our data analysis [12]. ... Figure 2: Windows Performance Monitoring the kernel yet tightly coupled to it. The plat- form library layer is next, followed by the appli- cation library, and finally the **application layer**. ...
Cited by 41 - Related articles - View as HTML - All 30 versions

☐ Create email alert

Gooooooooogle ▶

Result Page: 1 2 3 4 5 6 7 8 Next

"intrusion detection" "application lay(Search

Go to Google Home - About Google - About Google Scholar

©2011 Google